Security Target

McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6

Document Version 1.0

February 21, 2012

Prepared For:

McAfee, Inc.

2821 Mission College Blvd.

Santa Clara, CA 95054

www.mcafee.com

Prepared By:

Apex Assurance Group, LLC

530 Lytton Avenue, Ste. 200

Palo Alto, CA 94301

www.apexassurance.com

Abstract

This document provides the basis for an evaluation of a specific Target of Evaluation (TOE), the Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6. This Security Target (ST) defines a set of assumptions about the aspects of the environment, a list of threats that the product intends to counter, a set of security objectives, a set of security requirements and the IT security functions provided by the TOE which meet the set of requirements.

Table of Contents

List of Tables

List of Figures

1 Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), Security Target organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

ST Title	Security Target: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
ST Revision	1.0
ST Publication Date	February 21, 2012
Author	Apex Assurance Group

1.2 TOE Reference

TOE Reference	McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
TOE Type	Data Loss Prevention

1.3 Document Organization

This Security Target follows the following format:

SECTION	TITLE	DESCRIPTION
1	Introduction	Provides an overview of the TOE and defines the hardware and software that make up the TOE as well as the physical and logical boundaries of the TOE
2	Conformance Claims	Lists evaluation conformance to Common Criteria versions, Protection Profiles, or Packages where applicable
3	Security Problem Definition	Specifies the threats, assumptions and organizational security policies that affect the TOE
4	Security Objectives	Defines the security objectives for the TOE/operational environment and provides a rationale to demonstrate that the security objectives satisfy the threats
5	Extended Components Definition	Describes extended components of the evaluation (if any)
6	Security Requirements	Contains the functional and assurance requirements for this TOE
7	TOE Summary Specification	Identifies the IT security functions provided by the TOE and also identifies the assurance measures targeted to meet the assurance requirements.

Table 1 – ST Organization and Section Descriptions

1.4 Document Conventions

The notation, formatting, and conventions used in this Security Target are consistent with those used in Version 3.1 of the Common Criteria. Selected presentation choices are discussed here to aid the Security Target reader. The Common Criteria allows several operations to be performed on functional requirements: The allowable operations defined in Part 2 of the Common Criteria are *refinement, selection, assignment* and *iteration*.

- The assignment operation is used to assign a specific value to an unspecified parameter, such as the length of a password. An assignment operation is indicated by *italicized* text.
- The refinement operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Any text removed is indicated with a strikethrough format (Example: ~~TSF~~).
- The selection operation is picking one or more items from a list in order to narrow the scope of a component element. Selections are denoted by underlined text.
- Iterated functional and assurance requirements are given unique identifiers by appending to the base requirement identifier from the Common Criteria an iteration number inside parenthesis, for example, FIA_UAU.1.1 (1) and FIA_UAU.1.1 (2) refer to separate instances of the FIA_UAU.1 security functional requirement component.

Outside the SFRs, italicized text is used for both official document titles and text meant to be emphasized more than plain text.

1.5 Document Terminology

The following table[1] describes the terms and acronyms used in this document:

TERM	DEFINITION
AD	Active Directory
CC	Common Criteria version 3.1 (ISO/IEC 15408)
CPU	Central Processing Unit
DBMS	DataBase Management System
EAL	Evaluation Assurance Level
ePO	ePolicy Orchestrator
GUI	Graphical User Interface
I&A	Identification & Authentication
IIS	Internet Information Services
IP	Internet Protocol
IT	Information Technology

[1] Derived from the IDSPP

TERM	DEFINITION
JDBC	Java DataBase Connectivity
MAC	Media Access Control
MDAC	Microsoft Data Access Components
MSDE	MS Data Engine
NTFS	New Technology File System
NTP	Network Time Protocol
OEM	Original Equipment Manufacturer
OS	Operating System
OSP	Organizational Security Policy
PDC	Primary Domain Controller
PP	Protection Profile
RAM	Random Access Memory
SCAP	Security Content Automation Protocol
SF	Security Function
SFP	Security Function Policy
SFR	Security Functional Requirement
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Mail Protocol
SOF	Strength Of Function
SP	Service Pack
SQL	Structured Query Language
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSC	TOE Scope of Control
TSF	TOE Security Function
TSP	TOE Security Policy
VGA	Video Graphics Array
XML	eXtensible Markup Language

Table 2 – Terms and Acronyms Used in Security Target

1.6 TOE Overview

McAfee Host Data Loss Prevention software protects enterprises from the risk associated with unauthorized transfer of data from within or outside the organization. Data loss is defined as confidential or private information leaving the enterprise as a result of unauthorized communication through channels such as applications, physical devices, or network protocols.

Seamless integration with McAfee ePolicy Orchestrator® (ePO™) eases agent deployment, management, and reporting. ePO provides the user interface for the TOE via a GUI accessed from remote systems using web browsers. Custom reports can be fully automated, scheduled, or exported. ePO requires the user to identify and authenticate themselves before access is granted to any data or management functions. Audit records are generated to record configuration changes made by users. The audit records may be reviewed via the GUI. Users can review the results of the DLP policy audits via ePO and the Host DLP Monitor. Access to this information is again limited by per-user permissions.

The following sections provide a summary of the specific TOE sub-components. Note that communication between the distributed components of the TOE is protected from disclosure and modification by cryptographic functionality provided by the operational environment.

1.6.1 Host DLP Policy Manager Console

The Host DLP Policy Manager console is the interface where the administrator defines and enforces the enterprise information security policy. It is used to create the information security policy and administer the McAfee Host Data Loss Prevention components.

The Host DLP Policy Manager console is accessed from the ePolicy Orchestrator Menu and run locally on the administrative management workstation. Events that are generated by the DLP Agents are sent to the ePO Event Parser, and recorded in tables in the ePO database. Events are stored in the database for further analysis and used by other system components.

1.6.2 Host DLP Agent

The DLP Agents reside on enterprise computers, which are referred to as managed computers, and enforces the policies defined in the Host DLP Policy Manager. The agents audit user activities to monitor, control, and prevent unauthorized users from copying or transferring sensitive data. They also generate events recorded by the ePO Event Parser.

1.6.3 Host DLP Monitor

Events that are sent to the DLP Event Parser are displayed in the Host DLP Monitor, an interface accessed from the ePolicy Orchestrator Reporting console. All events can be filtered and sorted based on criteria such as protection rules, severity, date, time, user, computer name, or policy version. Events can be labeled by the administrator for tracking purposes.

1.7 TOE Description

McAfee Host Data Loss Prevention is a content-based agent solution that inspects enterprise users' actions concerning sensitive content in their own work environment, their computers. It uses advanced discovery technology as well as predefined dictionaries to identify this content, and incorporates device management and encryption for additional layers of control.

1.7.1 Physical Boundary

The TOE is a software TOE and includes:

1. The ePO application executing on a dedicated server

2. The Host DLP Monitor application on the same system as the ePO application
3. The McAfee Agent application on each managed system to be audited
4. The HDLP Agent software on each managed system to be audited

Note specifically that the hardware, operating systems and third party support software (e.g. DBMS) on each of the systems are excluded from the TOE boundary.

In order to comply with the evaluated configuration, the following hardware and software components should be used:

TOE COMPONENT	VERSION/MODEL NUMBER
TOE Software	Host DLP Monitor 9.2 Build 506 HDLP Agent Plug-In 9.2 Build 522 ePolicy Orchestrator 4.6.1 Build 1192 McAfee Agent 4.6[2] Build 1694
IT Environment	Specified in the following: • Table 4 – Management System Component Requirements • Table 5 – Supported Agent Platforms • Table 6 – Agent Platform Hardware Requirements

Table 3 – Evaluated Configuration for the TOE

The evaluated configuration consists of a single instance of the management system (with ePO and Host DLP Monitor) and one or more instances of managed systems (with McAfee Agent and the HDLP Agent Plug-in).

ePO supports both ePO authentication and Windows authentication of user account credentials. The evaluated configuration requires the use of Windows authentication only. User accounts (other than the password) are still required to be defined in ePO so that attributes can be associated with the account.

The following figure presents an example of an operational configuration. The shaded elements in the boxes at the top of the figure represent the TOE components.

[2] McAfee Agent 4.6 is shipped/packaged with ePO 4.6. From a clean installation, no additional steps are necessary to install McAfee Agent 4.6.

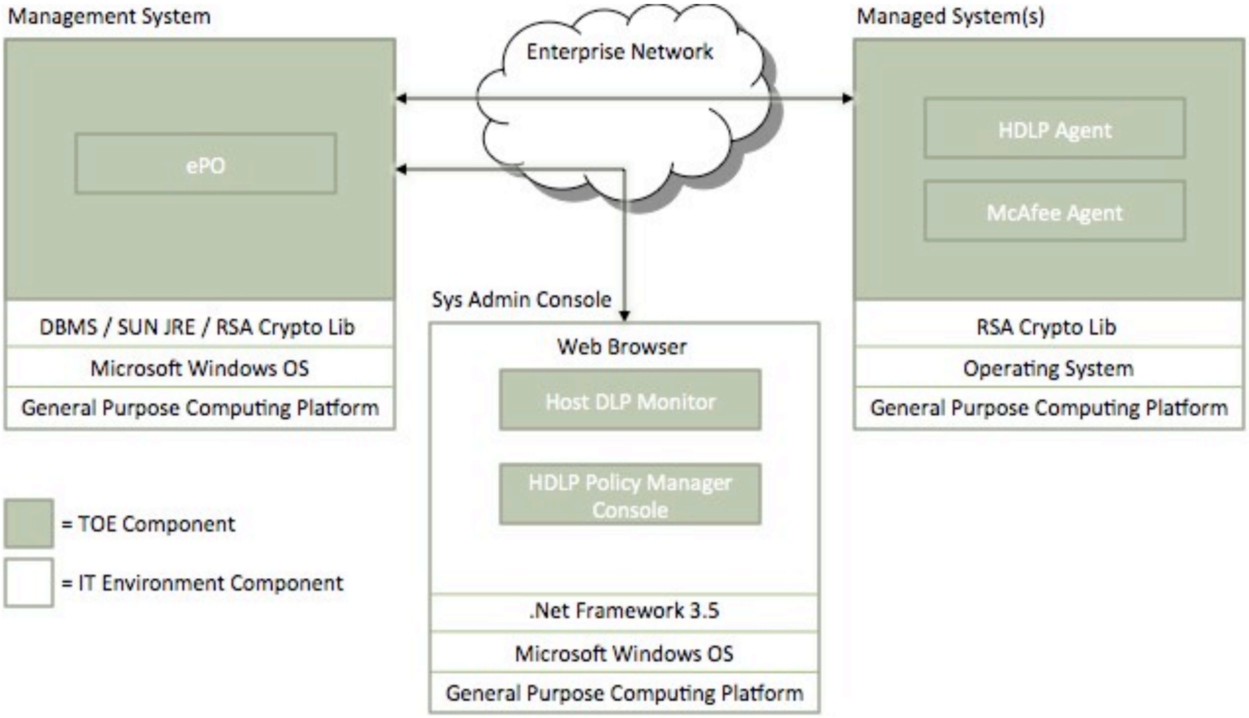

Figure 1 – TOE Boundary

The following specific configuration options apply to the evaluated configuration:

1. The McAfee Agent system tray icon is not displayed on managed systems.
2. McAfee Agent wake-up calls are enabled.
3. Incoming connections to McAfee Agents are only accepted from the configured address of the ePO server
4. The only repository supported is the ePO server.

1.7.2 Hardware and Software Supplied by the IT Environment

The TOE consists of a set of software applications. The hardware, operating systems and all third party support software (e.g., DBMS) on the systems on which the TOE executes are excluded from the TOE boundary.

The platform on which the ePO and Host DLP Monitor software is installed must be dedicated to functioning as the management system. ePO operates as a distribution system and management system for a client-server architecture offering components for the server part of the architecture (not the clients). The TOE requires the following hardware and software configuration on this platform.

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel Pentium III-class or higher; 1GHz or higher
Memory	1 GB RAM

COMPONENT	MINIMUM REQUIREMENTS
Processor	Intel Pentium 4-class or higher 1.3 GHz or higher
Memory	2 GB available RAM minimum 4 GB available RAM recommended minimum
Free Disk Space	1.5 GB — First-time installation minimum 2 GB — Upgrade minimum 2.5 GB — Recommended minimum
Monitor	1024x768, 256-color, VGA monitor or higher
Operating System	Windows Server 2003 Enterprise with Service Pack 2 or later Windows Server 2003 Standard with Service Pack 2 or later Windows Server 2003 Datacenter with Service Pack 2 or later Windows Server 2008 Enterprise with Service Pack 2 or later Windows Server 2008 Standard with Service Pack 2 or later Windows Server 2008 Datacenter with Service Pack 2 or later Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Standard Windows Server 2008 R2 Datacenter Windows 2008 Small Business Server Premium
Virtual Infrastructure	Citrix XenServer 5.5 Update 2 Microsoft Hyper-V Server 2008 R2 VMware ESX 3.5 Update 4 VMware ESX 4.0 Update 1
DBMS	Microsoft SQL Server 2005 (with Service Pack 3 or higher) Microsoft SQL Server 2008 SP1/SP2/R2
Network Card	Ethernet, 100Mb or higher
Disk Partition Formats	NTFS
Domain Controllers	The system must have a trust relationship with the Primary Domain Controller (PDC) on the network
Miscellaneous	Microsoft .NET Framework 2.0 or later (Required — You must acquire and install this software manually. This software is required if you select an installation option that automatically installs the SQL Server Express 2005 software bundled with this ePolicy Orchestrator software.) Microsoft updates Microsoft Visual C++ Required — Installed automatically. 2005 SP1 Redistributable Microsoft Visual C++ Required — Installed automatically. 2008 Redistributable Package (x86) MSXML 6.0

Table 4 – Management System Component Requirements

The McAfee Agent and HDLP Agent Plug-In execute on one or more systems whose policy settings are to be audited. The supported platforms for these components are:

SUPPORTED AGENT OS	PLATFORM
Windows 2000 Server with SP 1, 2, 3, or 4	X86 platforms
Windows 2000 Advanced Server with SP 1, 2, 3, or 4	X86 platforms

SUPPORTED AGENT OS	PLATFORM
Windows 2000 Professional with SP 1, 2, 3, or 4	X86 platforms
Windows XP Professional with SP1	X86 and X64 platforms
Windows Server 2003 Standard Edition	X86 and X64 platforms
Windows Server 2003 Enterprise Edition	X86 and X64 platforms
Windows Vista, 7	X86 and X64 platforms
Windows 2008 Server	X86 and X64 platforms

Table 5 – Supported Agent Platforms

The minimum hardware requirements for the agent platforms are specified in the following table:

COMPONENT	MINIMUM HARDWARE REQUIREMENTS
Memory	20MB RAM
Free Disk Space	80MB
Network Card	Ethernet, 10Mb or higher

Table 6 – Agent Platform Hardware Requirements

The management system is accessed from remote systems via a browser. The supported browsers are Microsoft Internet Explorer 6.0 with Service Pack 1 or later or Microsoft Internet Explorer 7.0.

The TOE relies on Windows to authenticate user credentials during the logon process. User accounts must also be defined within ePO in order to associate permissions with the users.

1.7.3 Logical Boundary

This section outlines the boundaries of the security functionality of the TOE; the logical boundary of the TOE includes the security functionality described in the following sections.

TSF	DESCRIPTION
Policy Enforcement	The TOE enforces policies on managed systems and audits end-user action against those policies. The TOE ensures end users aren't allowed to copy/modify files as specified by an administrator through a data loss prevention policy. Systems events and alerts are stored in the database (the DBMS is in the IT Environment), and reports based upon completed policy audits may be retrieved via the GUI interface.
Identification	On the management system, the TOE requires users to identify and authenticate themselves before accessing the TOE software. User accounts must be defined within ePO, but authentication of the user credentials is performed by Windows. No action can be initiated before proper identification and authentication. Each TOE user has security attributes associated with their user account that define the functionality the user is allowed to perform. On the management system and all managed systems, I&A for local login to the operating system (i.e., via a local console) is performed by the local OS (IT Environment).

TSF	DESCRIPTION
Management	The TOE's Management Security Function provides support functionality that enables users to configure and manage TOE components. Management of the TOE may be performed via the GUI. Management privileges are defined per-user.
Audit	The TOE's Audit Security Function provides auditing of management actions performed by administrators. Authorized users may review the audit records via ePO.
System Information Import	The TOE may be configured to import information about systems to be managed from Active Directory (LDAP servers) or NT domain controllers. This functionality ensures that all the defined systems in the enterprise network are known to the TOE and may be configured to be managed.

Table 7 – Logical Boundary Descriptions

1.7.3.1 TOE Guidance

The following guidance documentation is provided as part of the TOE:

- *Operational User Guidance and Preparative Procedures Supplement: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6*
- *Installation Guide: McAfee® Data Loss Prevention 9.2 Software For Use with ePolicy Orchestrator® 4.6.0 Software*
- *Product Guide: McAfee Data Loss Prevention 9.2 Software For Use with ePolicy Orchestrator® 4.6.0 Software*
- *Installation Guide McAfee ePolicy Orchestrator 4.6.0 Software*

1.8 Rationale for Non-bypassability and Separation of the TOE

The responsibility for non-bypassability and non-interference is split between the TOE and the IT Environment. TOE components are software only products and therefore the non-bypassability and non-interference claims are dependent upon hardware and OS mechanisms. The TOE runs on top of the IT Environment supplied operating systems.

The TOE ensures that the security policy is applied and succeeds before further processing is permitted whenever a security relevant interface is invoked: the interfaces are well defined and insure that the access restrictions are enforced. Non-security relevant interfaces do not interact with the security functionality of the TOE. The TOE depends upon OS mechanisms to protect TSF data such that it can only be accessed via the TOE. The systems on which the ePO, Host DLP Monitor, and HDLP Policy Manager TOE components execute are dedicated to that purpose.

The TOE is implemented with well-defined interfaces that can be categorized as security relevant or non-security relevant. The TOE is implemented such that non-security relevant interfaces have no means of impacting the security functionality of the TOE. Unauthenticated users may not perform any actions within the TOE. The TOE tracks multiple users by sessions and ensures the access privileges of each are enforced.

The server hardware provides virtual memory and process separation, which the server OS utilizes to ensure that other (non-TOE) processes may not interfere with the TOE; all interactions are limited to the defined TOE interfaces. The OS and DBMS restrict access to TOE data in the database to prevent interference with the TOE via that mechanism.

The TOE consists of distributed components. Communication between the components relies upon cryptographic functionality provided by the OS or third party software (operational environment) to protect the information exchanged from disclosure or modification.

2 Conformance Claims

2.1 Common Criteria Conformance Claim

The TOE is Common Criteria Version 3.1 Revision 3 (July 2009) Part 2 conformant and Part 3 conformant at Evaluation Assurance Level 2 and augmented by ALC_FLR.2 – Flaw Reporting Procedures.

2.2 Protection Profile Conformance Claim

The TOE does not claim conformance to a Protection Profile.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organizational security policy statements or rules with which the TOE must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

This chapter identifies assumptions as A.*assumption*, threats as T.*threat* and policies as P.*policy*.

3.1 Threats

The following are threats identified for the TOE and the IT System the TOE monitors. The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker for all the threats is unsophisticated.

The TOE addresses the following threats:

THREAT	DESCRIPTION
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism.
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data
T.SENSITIVE_DATA	An unauthorized user may transmit or transfer sensitive data from managed systems.

Table 8 – Threats Addressed by the TOE

3.2 Organizational Security Policies

An organizational security policy is a set of rules, practices, and procedures imposed by an organization to address its security needs. The following Organizational Security Policies apply to the TOE:

POLICY	DESCRIPTION

POLICY	DESCRIPTION
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes.
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected.
P.IMPORT	The TOE shall be able to import data about managed systems from LDAP servers and NT Domains.
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification.
P.MANAGE	The TOE shall only be managed by authorized users.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions.

Table 9 – Organizational Security Policies

3.3 Assumptions

This section describes the security aspects of the environment in which the TOE is intended to be used. The TOE is assured to provide effective security measures in a co-operative non-hostile environment only if it is installed, managed, and used correctly. The following specific conditions are assumed to exist in an environment where the TOE is employed.

ASSUMPTION	DESCRIPTION
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions.
A.ASCOPE	The TOE is appropriately scalable to the IT Systems the TOE monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification.

Table 10 – Assumptions

4 Security Objectives

4.1 Security Objectives for the TOE

The IT security objectives for the TOE are addressed below:

OBJECTIVE	DESCRIPTION
O.ACCESS	The TOE must allow authorized users to access only authorized TOE functions and data.
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system.
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information generated by the TOE.
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data.
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE functions and data on the management system.
O.IMPORT	The TOE shall provide mechanisms to import system data from Active Directory (LDAP servers) and NT Domain Controllers.
O.INTEGRITY	The TOE must ensure the integrity of all System data.
O.SENSITIVE_DATA	The TOE shall take specified actions upon the access, transmission, printing, or copying of sensitive files or data.

Table 11 – TOE Security Objectives

4.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are addressed below:

OBJECTIVE	DESCRIPTION
OE.PHYCAL	Those responsible for the TOE must ensure that those parts of the TOE critical to security policy are protected from any physical attack.
OE.CREDEN	Those responsible for the TOE must ensure that all access credentials are protected by the users in a manner which is consistent with IT security.
OE.INSTALL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which is consistent with IT security.
OE.INTEROP	The TOE is interoperable with the managed systems it monitors
OE.PERSON	Personnel working as authorized administrators shall be carefully selected and trained for proper operation of the System.
OE.AUDIT_PROTECT	The IT Environment will provide the capability to protect audit information generated by the TOE via mechanisms outside the TSC.
OE.AUDIT_REVIEW	The IT Environment will provide the capability for authorized administrators to review audit information generated by the TOE.

OBJECTIVE	DESCRIPTION
OE.CRYPTO	The IT Environment will provide the cryptographic functionality and protocols required for the TOE to securely transfer information between distributed portions of the TOE.
OE.DATABASE	Those responsible for the TOE must ensure that access to the database via mechanisms outside the TOE boundary (e.g., DBMS) is restricted to authorized users only.
OE.IDAUTH	The IT Environment must be able to identify and authenticate users prior to them gaining access to TOE functionality on the managed system. It must also be able to authenticate user credentials on the management system when requested by the TOE.
OE.PROTECT	The IT environment will protect itself and the TOE from external interference or tampering.
OE.SD_PROTECTION	The IT Environment will provide the capability to protect system data via mechanisms outside the TSC.
OE.STORAGE	The IT Environment will store TOE data in the database and retrieve it when directed by the TOE.
OE.TIME	The IT Environment will provide reliable timestamps to the TOE

Table 12 – Operational Environment Security Objectives

4.3 Security Objectives Rationale

This section provides the summary that all security objectives are traced back to aspects of the addressed assumptions, threats, and Organizational Security Policies (if applicable). The following table provides a high level mapping of coverage for each threat, assumption, and policy:

OBJECTIVE THREAT / ASSUMPTION	O.EADMIN	O.ACCESS	O.IDENTIFY	O.INTEGRITY	OE.INSTALL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTEROP	O.AUDITS	O.AUDIT_PROTECT	O.IMPORT	O.SENSITIVE_DATA	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.CRYPTO	OE.STORAGE
A.ACCESS									✓													
A.ASCOPE									✓													
A.DATABASE																		✓				
A.DYNMIC								✓	✓													
A.LOCATE						✓																
A.MANAGE								✓														
A.NOEVIL					✓	✓	✓															
A.PROTCT						✓																
P.ACCACT			✓							✓							✓			✓		
P.ACCESS		✓	✓													✓	✓	✓				
P.DETECT										✓				✓								
P.IMPORT												✓										
P.INTEGRITY				✓							✓								✓		✓	✓
P.MANAGE	✓	✓	✓		✓		✓	✓									✓					

OBJECTIVE THREAT / ASSUMPTION	O.EADMIN	O.ACCESS	O.IDENTIFY	O.INTEGRITY	OE.INSTALL	OE.PHYCAL	OE.CREDEN	OE.PERSON	OE.INTEROP	O.AUDITS	O.AUDIT_PROTECT	O.IMPORT	O.SENSITIVE_DATA	OE.TIME	OE.PROTECT	OE.SD_PROTECTION	OE.IDAUTH	OE.DATABASE	OE.AUDIT_PROTECT	OE.AUDIT_REVIEW	OE.CRYPTO	OE.STORAGE
P.PROTCT						✓									✓						✓	✓
T.COMDIS		✓	✓												✓		✓					
T.COMINT		✓	✓	✓											✓		✓					
T.IMPCON	✓	✓	✓		✓												✓					
T.LOSSOF		✓	✓	✓													✓					
T.NOHALT		✓	✓														✓					
T.PRIVIL		✓	✓														✓					
T.SENSITIVE_ DATA													✓									

Table 13 – Mapping of Assumptions, Threats, and OSPs to Security Objectives

The following table provides detailed evidence of coverage for each threat, policy, and assumption:

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.ACCESS	The TOE has access to all the IT System data it needs to perform its functions. The OE.INTEROP objective ensures the TOE has the needed access.
A.ASCOPE	The TOE is appropriately scalable to the IT System the TOE monitors. The OE.INTEROP objective ensures the TOE has the necessary interactions with the IT System it monitors.
A.DATABASE	Access to the database used by the TOE via mechanisms outside the TOE boundary is restricted to use by authorized users. The OE.DATABASE objective ensures that access to any mechanisms outside the TOE boundary that may be used to access the database is configured by the administrators such that only authorized users may utilize the mechanisms.
A.DYNMIC	The TOE will be managed in a manner that allows it to appropriately address changes in the IT System the TOE monitors. The OE.INTEROP objective ensures the TOE has the proper access to the IT System. The OE.PERSON objective ensures that the TOE will managed appropriately.
A.LOCATE	The processing resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access. The OE.PHYCAL provides for the physical protection of the TOE.
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. The OE.PERSON objective ensures all authorized administrators are qualified and trained to manage the TOE.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
A.NOEVIL	The authorized administrators are not careless, willfully negligent, or hostile, and will follow and abide by the instructions provided by the TOE documentation. The OE.INSTALL objective ensures that the TOE is properly installed and operated and the OE.PHYCAL objective provides for physical protection of the TOE by authorized administrators. The OE.CREDEN objective supports this assumption by requiring protection of all authentication data.
A.PROTCT	The TOE hardware and software critical to security policy enforcement will be protected from unauthorized physical modification. The OE.PHYCAL provides for the physical protection of the TOE hardware and software.
P.ACCACT	Users of the TOE shall be accountable for their actions within the TOE. The O.AUDITS objective implements this policy by requiring auditing of all data accesses and use of TOE functions. The O.IDENTIFY objective supports this objective by ensuring each user is uniquely identified. The OE.IDAUTH objective supports this objective by ensuring each user is uniquely identified and authenticated. The OE.AUDIT_REVIEW objective provides the ability for administrators to review the audit records generated by the TOE so that accountability for administrator actions can be determined.
P.ACCESS	All data collected and produced by the TOE shall only be used for authorized purposes. The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses via the ePO web interface. The OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTIFY and OE.IDAUTH objectives by only permitting authorized users to access TOE functions. The OE.SD_PROTECTION and OE.DATABASE objectives counter this threat for mechanisms outside the TSC via IT Environment protections of the system data trail and the database used to hold TOE data. The OE.SD_PROTECTION and O.ACCESS objectives counter this threat for mechanisms inside the TSC via TOE protections of the system data trail and the database used to hold TOE data.
P.DETECT	Static configuration information that might be indicative of the potential for a future intrusion or the occurrence of a past intrusion of an IT System or events that are indicative of inappropriate activity that may have resulted from misuse, access, or malicious activity of IT System assets must be collected. The O.AUDITS objectives address this policy by requiring collection of audit and policy audit data. The OE.TIME objective supports this policy by providing a time stamp for insertion into the system data records.
P.IMPORT	The TOE shall be able to import data about managed systems from LDAP servers and NT Domains. The O.IMPORT objective addresses this policy by requiring the TOE to provide functionality to import data about managed systems from LDAP servers and NT Domains.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
P.INTEGRITY	Data collected and produced by the TOE shall be protected from modification. The O.INTEGRITY objective ensures the protection of System data from modification. The O.AUDIT_PROTECT and OE.AUDIT_PROTECT objectives ensure the integrity of audit records in the database generated by the TOE using access mechanisms inside and outside the TSC respectively. The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
P.MANAGE	The TOE shall only be managed by authorized users. The OE.PERSON objective ensures competent administrators will manage the TOE and the O.EADMIN objective ensures there is a set of functions for administrators to use. The OE.INSTALL objective supports the OE.PERSON objective by ensuring administrator follow all provided documentation and maintain the security policy. The O.IDENTIFY objective provides for identification of users prior to any TOE function accesses. The OE.IDAUTH objective provides for authentication of users prior to any TOE function accesses. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions. The OE.CREDEN objective requires administrators to protect all authentication data.
P.PROTCT	The TOE shall be protected from unauthorized accesses and disruptions of TOE data and functions. The OE.PHYCAL objective protects the TOE from unauthorized physical modifications. The OE.PROTECT objective supports the TOE protection from the IT Environment. The OE.CRYPTO objective requires the IT Environment to provide cryptographic functionality and protocols that can be used by the TOE to protect the data during transit. The OE.STORAGE objective requires the IT Environment to provide storage and retrieval mechanisms for System data for use by the TOE.
T.COMDIS	An unauthorized user may attempt to disclose the data collected and produced by the TOE by bypassing a security mechanism. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The OE.PROTECT objective supports the TOE protection from the IT Environment.
T.COMINT	An unauthorized user may attempt to compromise the integrity of the data collected and produced by the TOE by bypassing a security mechanism. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The O.INTEGRITY objective ensures no System data will be modified. The OE.PROTECT objective supports the TOE protection from the IT Environment.

THREATS, POLICIES, AND ASSUMPTIONS	RATIONALE
T.IMPCON	An unauthorized user may inappropriately change the configuration of the TOE causing potential intrusions to go undetected. The OE.INSTALL objective states the authorized administrators will configure the TOE properly. The O.EADMIN objective ensures the TOE has all the necessary administrator functions to manage the product. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.
T.LOSSOF	An unauthorized user may attempt to remove or destroy data collected and produced by the TOE. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE data. The O.INTEGRITY objective ensures no System data will be deleted.
T.NOHALT	An unauthorized user may attempt to compromise the continuity of the System's collection and analysis functions by halting execution of the TOE. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.
T.PRIVIL	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. The O.IDENTIFY objective provides for identification of users prior to any TOE data access. The OE.IDAUTH objective provides for authentication of users prior to any TOE data access. The O.ACCESS objective builds upon the O.IDENTIFY objective by only permitting authorized users to access TOE functions.
T.SENSITVE_DATA	An unauthorized user may transmit or transfer sensitive data from managed systems. The O.SENSITIVE_DATA objective requires the TOE to take specified actions upon the access, transmission, printing, or copying of sensitive files or data.

Table 14 – Rationale for Mapping of Threats, Policies, and Assumptions to Objectives

5 Extended Components Definition

This Security Target does not include any extended components.

6 Security Requirements

The security requirements that are levied on the TOE and the IT environment are specified in this section of the ST.

6.1 Security Functional Requirements

The functional security requirements for this Security Target consist of the following components from Part 2 of the CC, and those that were explicitly stated, all of which are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
Security Audit	FAU_GEN.1	Audit Data Generation
	FAU_GEN.2	User Identity Association
	FAU_SAR.1	Audit Review
	FAU_SAR.2	Restricted Audit Review
	FAU_STG.1	Protected Audit Trail Storage
Information Flow Control	FDP_IFC.1	Subset Information Flow Control
	FDP_IFF.1	Simple Security Attributes
Identification and Authentication	FIA_ATD.1	User Attribute Definition
	FIA_UID.1	Timing of Identification
	FIA_USB.1	User-Subject Binding
Security Management	FMT_MTD.1	Management of TSF Data
	FMT_SMF.1	Specification of Management Functions
	FMT_SMR.1	Security Roles
Protection of the TSF	FPT_TDC.1	Inter-TSF Basic TSF Data Consistency

Table 15 – TOE Functional Components

6.1.1 Security Audit (FAU)

6.1.1.1 FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the not specified level of audit; and

c) *The events identified in* Table 16 – Audit Events and Details

FAU_GEN.1.2 The TSF shall record within each audit record at last the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, *the information detailed in*

Table 16 – Audit Events and Details.

Application Note: The auditable events for the (not specified) level of auditing are included in the following table:

COMPONENT	EVENT	DETAILS
FAU_GEN.1	Start-up and shutdown of audit functions	
FAU_GEN.1	Access to the TOE and System data	Object IDs, Requested access
FAU_SAR.1	Reading of information from the audit records.	
FDP_IFF.1	All decisions on requests for information flow.	The presumed addresses of the source and destination subject.
FAU_SAR.2	Note: Unsuccessful attempts to read information from the audit records do not occur because the TOE does not present that capability to users that are not authorized to read the audit records.	
FIA_ATD.1	All changes to TSF data (including passwords) result in an audit record being generated. Note that passwords are not configured, so no audit records for rejection of a tested secret will be generated.	
FIA_UID.1	All use of the user identification mechanism	User identity, location
FIA_USB.1	Successful binding of attributes to subjects is reflected in the audit record for successful authentication. Unsuccessful binding does not occur in the TOE design.	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_SMF.1	Use of the management functions.	User identity, function used
FMT_SMR.1	Modifications to the group of users that are part of a role	User identity
FPT_TDC.1	Use of the asset import function	Data Source, result, identification of which TSF data have been imported
	Detection of modified TSF data	Data Source, Identification of which TSF data have been modified

Table 16 – Audit Events and Details

6.1.1.2 FAU_GEN.2 User Identity Association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.1.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The TSF shall provide *authorized users with Global Administrator status or the View Audit Log permission* with the capability to read *all information* from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.1.1.5 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail.

6.1.2 Information Flow Control (FDP)

6.1.2.1 FDP_IFC.1 – Subset Information Flow Control

FDP_IFC.1.1 The TSF shall enforce the *DLP Information Flow Control SFP* on

Subjects: External IT entities attempting to transfer or transmit sensitive data

Information: Files and content stored on the managed system or transferred from the managed system

Operations: Apply RM policy, Block, Encrypt, Delete, Monitor, Notify User, Quarantine, Read Only, Request Justification, Store Evidence.

6.1.2.2 FDP_IFF.1 – Simple Security Attributes

FDP_IFF.1.1 The TSF shall enforce the *DLP Information Flow Control SFP* based on the following types of subject and information security attributes:

Subject Security Attributes:

- *IP Address*

- *MAC Address*
- *Agent ID*
- *User Assignment Group*
- *Computer Assignment Group*

Information Security Attributes

- *Application*
- *Dictionary*
- *Email Destination*
- *File Extension*
- *File Server*
- *Network*
- *Printer*
- *Registered document repository*
- *Tag/Content Category*
- *Text Pattern*
- *Web Destination*
- *Whitelist*
- *Associated Protection Rules*.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

A. Monitoring option is enabled for the service and information structure type AND:

1. *The attribute is not covered by protection rule OR*
2. *The attribute is whitelisted.*

OR

B. DLP monitoring is disabled for the subject and information structure type.

FDP_IFF.1.3 The TSF shall enforce ~~the~~ *no other additional rules.*

FDP_IFF.1.4 The TSF shall explicitly authorize an information flow based on the following rules: *No explicit authorization rules*.

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: *No explicit denial rules*.

6.1.3 Identification and Authentication (FIA)

6.1.3.1 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

a) ePO User name;

b) Enabled or disabled;

c) Authentication configuration (must be configured for Windows);

d) Global Administrator status; and

e) *Permission Sets.*

6.1.3.2 FIA_UID.1 Timing of Identification

FIA_UID.1.1 The TSF shall allow *no actions* on behalf of the user to be performed **on the management system** before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user **on the management system**.

Application Note and Refinement Rationale: The TOE performs identification on the management system then relies upon Windows for authentication.

Application Note: Authentication on the managed systems is the responsibility of the operating environment.

6.1.3.3 FIA_USB.1 User-Subject Binding

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on behalf of that user:

a) Global Administrator status; and

b) Permissions.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: *user security attributes are bound upon successful login with a valid ePO User Name*.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: *user security attributes do not change until the user refreshes the menu of the GUI management session*.

Application Note: Permissions are determined by the union of all permissions in any permission set associated with a user.

Application Note: If the security attributes for a user are changed while that user has an active session, the new security attributes are not bound to a session until the next page refresh.

6.1.4 Security Management (FMT)

6.1.4.1 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, clear, *create, export and use* the *TSF data identified in* Table 17 – TSF Data Access Permissions *to a Global Administrator or a user with appropriate permissions*.

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
Contacts	Create and edit contacts	Query, create, delete and modify
	Use contacts	Use
Dashboards	Use public dashboards	Query and use public dashboards
	Use public dashboards; create and edit personal dashboards	Query and use public dashboards; create and modify personal dashboards
	Use public dashboards; create and edit personal dashboards; make personal dashboards public	Query and use public dashboards; create, delete and modify personal dashboards; make personal dashboards public
Data Retention Settings	n/a (only allowed by a Global Administrator)	Query and modify
Email Servers	n/a (only allowed by a Global Administrator)	Query, create, delete and modify
Event Records (DLP Policies)	Add, remove and change Audits and Assignments	Query DLP policy audit event records
	View Audits and Assignments	Query DLP policy audit event records

TSF DATA	ASSOCIATED PERMISSION	OPERATIONS PERMITTED
ePO User Accounts	n/a (only allowed by a Global Administrator)	Query, create, delete and modify
Event Filtering	n/a (only allowed by a Global Administrator)	Query and modify
Global Administrator Status	n/a (only allowed by a Global Administrator)	Query and modify
Groups	View "System Tree" tab	Query
	View "System Tree" tab along with Edit System Tree groups and systems	Query, create, delete and modify
Notification Rules	View notification rules and Notification Log	Query
	Create and edit notification rules; view Notification Log	Query, create, delete and modify
	Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers and external commands	Query, create, delete and modify
Permission Set	n/a (only allowed by a Global Administrator)	Query, create, delete, modify, and assign (to a user) permissions
Protection Rules	View settings	Query
	View and change settings	Query, create, delete, and modify (including enable)
Queries	Use public queries	Query and use public queries
	Use public queries; create and edit personal queries	Query and use public queries; create and modify personal queries
	Edit public queries; create and edit personal queries; make personal queries public	Query, delete, modify and use public queries; create, delete and modify (including make public) personal queries
Server Settings	n/a (only allowed by a Global Administrator)	Query and modify
System Information	Create and edit systems	Query, create, delete and modify
System Tree	View System Tree	Query

Table 17 – TSF Data Access Permissions

6.1.4.2 FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1 The TSF shall be capable of performing the following **security** management functions:

a) ePO User Account management,

b) Permission Set management,

c) Audit Log management,

d) Event Log management,

e) Notification management,

f) Event Filtering management,

g) System Tree management,

h) DLP Policy and Rule management,

i) Query management,

j) Dashboard management.

6.1.4.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 The TSF shall maintain the roles: *Global Administrator and User*.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application Note: A Global Administrator is a defined user account with Global Administrator status. Users are defined user accounts without Global Administrator status but with specific permissions.

6.1.5 Protection of the TSF (FPT)

6.1.5.1 FPT_TDC.1 Inter-TSF Basic TSF Data Consistency

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret *system information* when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use *the following rules* when interpreting the TSF data from another trusted IT product.

a) For Active Directory (LDAP servers), the data is interpreted according to the LDAP version 3 protocol.

b) For NT Domains, the data is interpreted according to the NetBIOS protocol.

c) When conflicting information is received from different sources, highest priority is given to information learned from the McAfee Agent, then to Active Directory, and finally to NT Domains.

6.2 Security Assurance Requirements

The assurance security requirements for this Security Target are taken from Part 3 of the CC. These assurance requirements compose an Evaluation Assurance Level 2 (EAL2) augmented by ALC_FLR.2. The assurance components are summarized in the following table:

CLASS HEADING	CLASS_FAMILY	DESCRIPTION
ADV: Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
AGD: Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative Procedures
ALC: Lifecycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting Procedures
ATE: Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional Testing
	ATE_IND.2	Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

Table 18 – Security Assurance Requirements at EAL2

6.3 CC Component Hierarchies and Dependencies

This section of the ST demonstrates that the identified SFRs include the appropriate hierarchy and dependencies. The following table lists the TOE SFRs and the SFRs each are hierarchical to, dependent upon and any necessary rationale.

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FAU_GEN.1	No other components	FPT_STM.1	Satisfied by OE.TIME in the environment
FAU_GEN.2	No other components	FAU_GEN.1, FIA_UID.1	Satisfied Satisfied
FAU_SAR.1	No other components	FAU_GEN.1	Satisfied
FAU_SAR.2	No other components	FAU_SAR.1	Satisfied
FAU_STG.1	No other components	FAU_GEN.1	Satisfied
FDP_IFC.1	No other components	FDP_IFF.1	Satisfied
FDP_IFF.1	No other components	FDP_IFC.1 FMT_MSA.3	Satisfied[3]

[3] FMT_MSA.3 does not impact the security required by FDP_IFF.1 for this particular TOE because there are no configurable security attributes

SFR	HIERARCHICAL TO	DEPENDENCY	RATIONALE
FIA_ATD.1	No other components	None	n/a
FIA_UID.1	No other components	None	n/a
FIA_USB.1	No other components	FIA_ATD.1	Satisfied
FMT_MTD.1	No other components	FMT_SMF.1 FMT_SMR.1	Satisfied Satisfied
FMT_SMF.1	No other components	None	n/a
FMT_SMR.1	No other components	FIA_UID.1	Satisfied
FPT_TDC.1	No other components	None	n/a

Table 19 – TOE SFR Dependency Rationale

6.4 Security Requirements Rationale

This section provides rationale for the Security Functional Requirements demonstrating that the SFRs are suitable to address the security objectives

6.4.1 Security Functional Requirements for the TOE

The following table provides a high level mapping of coverage for each security objective:

OBJECTIVE SFR	O.ACCESS	O.AUDITS	O.AUDIT_PROTECT	O.EADMIN	O.IDENTIFY	O.IMPORT	O.INTEGRITY	O.SENSITIVE_DATA
FAU_GEN.1		✓						
FAU_GEN.2		✓						
FAU_SAR.1	✓							
FAU_SAR.2	✓							
FAU_STG.1		✓	✓					
FDP_IFC.1								✓
FDP_IFF.1								✓
FIA_ATD.1					✓			
FIA_UID.1	✓				✓			
FIA_USB.1	✓							
FMT_MTD.1	✓			✓		✓	✓	
FMT_SMF.1	✓			✓				
FMT_SMR.1	✓			✓				

OBJECTIVE / SFR	O.ACCESS	O.AUDITS	O.AUDIT_PROTECT	O.EADMIN	O.IDENTIFY	O.IMPORT	O.INTEGRITY	O.SENSITIVE_DATA
FPT_TDC.1						✓		

Table 20 – Mapping of TOE SFRs to Security Objectives

The following table provides detailed evidence of coverage for each security objective:

OBJECTIVE	RATIONALE
O.ACCESS	The TOE must allow authorized users to access only appropriate TOE functions and data. Users authorized to access the TOE are determined using an identification process [FIA_UID.1]. Upon successful I&A, the security attributes for the user are bound to the subject so that proper access controls can be enforced [FIA_USB.1]. The permitted access to TOE data by the roles and permissions is defined [FMT_MTD.1, FMT_SMF.1, FMT_SMR.1]. The audit log records may only be viewed by authorized users (FAU_SAR.1, FAU_SAR.2].
O.AUDITS	The TOE must record audit records for data accesses and use of the TOE functions on the management system. Security-relevant events must be defined and auditable for the TOE [FAU_GEN.1]. The user associated with the events must be recorded [FAU_GEN.2]. The TOE does not provide any mechanism for users to modify or delete audit records other than via configuration of the data retention timeframe, and that functionality is limited to administrators [FAU_STG.1].
O.AUDIT_PROTECT	The TOE will provide the capability to protect audit information generated by the TOE. The TOE is required to protect the stored audit records from unauthorized deletion or modification [FAU_STG.1].
O.EADMIN	The TOE must include a set of functions that allow effective management of its functions and data. The functions and roles required for effective management are defined [FMT_SMF.1, FMT_SMR.1], and the specific access privileges for the roles and permissions is enforced [FMT_MTD.1].
O.IDENTIFY	The TOE must be able to identify users prior to allowing access to TOE functions and data on the management system. Security attributes of subjects used to enforce the security policy of the TOE must be defined [FIA_ATD.1]. Users authorized to access the TOE are determined using an identification process [FIA_UID.1] and the TOE relies upon authentication services provided by the operational environment.

OBJECTIVE	RATIONALE
O.IMPORT	The TOE shall provide mechanisms to import system information from Active Directory (LDAP servers) and NT Domains. The TOE defines management functionality to import system tree information [FMT_MTD.1] and the rules for interpreting data from those sources [FPT_TDC.1].
O.INTEGRITY	The TOE must ensure the integrity of all System data. Only authorized administrators of the System may query or add System data [FMT_MTD.1].
O.SENSITIVE_DATA	The TOE shall take specified actions upon the access, transmission, printing, or copying of sensitive files or data. The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is handled inappropriately [FDP_IFC.1 and FDP_IFF.1].

Table 21 – Rationale for Mapping of TOE SFRs to Objectives

6.4.2 Security Assurance Requirements

This section identifies the Lifecycle , Development, Test, and Guidance measures applied to satisfy CC assurance requirements.

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ADV_ARC.1: Security Architecture Description	Architecture Description: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
ADV_FSP.2: Security-Enforcing Functional Specification	Functional Specification: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
ADV_TDS.1: Basic Design	Basic Design: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
AGD_OPE.1: Operational User Guidance	Operational User Guidance and Preparative Procedures Supplement: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
AGD_PRE.1: Preparative Procedures	Operational User Guidance and Preparative Procedures Supplement: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
ALC_CMC.2: Use of a CM System	Configuration Management Processes and Procedures: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
ALC_CMS.2: Parts of the TOE CM Coverage	Configuration Management Processes and Procedures: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
ALC_DEL.1: Delivery Procedures	Delivery Procedures: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
ALC_FLR.2: Flaw Reporting	Flaw Reporting: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
ATE_COV.1: Evidence of Coverage	Security Testing: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6

SECURITY ASSURANCE REQUIREMENT	ASSURANCE MEASURES / EVIDENCE TITLE
ATE_FUN.1: Functional Testing	Security Testing: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
ATE_IND.2: Independent Testing – Sample	Security Testing: McAfee Host Data Loss Prevention 9.2 and ePolicy Orchestrator 4.6
AVA_VAN.2: Vulnerability Analysis	Performed and provided by CCTL

Table 22 – Security Assurance Measures

6.4.2.1 Rationale for TOE Assurance Requirements Selection

The TOE stresses assurance through vendor actions that are within the bounds of current best commercial practice. The TOE provides, via review of vendor-supplied evidence, independent confirmation that these actions have been competently performed.

The general level of assurance for the TOE is:

1. Consistent with current best commercial practice for IT development and provides a product that is competitive against non-evaluated products with respect to functionality, performance, cost, and time-to-market.
2. The TOE assurance also meets current constraints on widespread acceptance, by expressing its claims against EAL2 from part 3 of the Common Criteria.
3. Consistent with current best practice for tracking and fixing flaws as well as providing fixes to customers.

6.5 TOE Summary Specification Rationale

This section demonstrates that the TOE's Security Functions completely and accurately meet the TOE SFRs.

The following tables provide a mapping between the TOE's Security Functions and the SFRs and the rationale.

TSF SFR	Policy Enforcement	Identification	Management	Audit	System Information Import
FAU_GEN.1				✓	
FAU_GEN.2				✓	
FAU_SAR.1				✓	
FAU_SAR.2				✓	
FAU_STG.1				✓	

TSF SFR	Policy Enforcement	Identification	Management	Audit	System Information Import
FDP_IFC.1	✓				
FDP_IFF.1	✓				
FIA_ATD.1			✓		
FIA_UID.1		✓			
FIA_USB.1		✓			
FMT_MTD.1			✓		
FMT_SMF.1			✓		
FMT_SMR.1			✓		
FPT_TDC.1					✓

Table 23 – SFR to TOE Security Functions Mapping

SFR	SF AND RATIONALE
FAU_GEN.1	**Audit –** ePO user actions area audited according to the events specified in the table with the SFR.
FAU_GEN.2	**Audit –** The audit log records include the associated user name when applicable.
FAU_SAR.1	**Audit –** Audit log records are displayed in a human readable table form from queries generated by authorized users.
FAU_SAR.2	**Audit –** Only authorized users have permission to query audit log records.
FAU_STG.1	**Audit –** The only mechanism provided by the TOE to cause audit records to be deleted is configuration of the data retention timeframe, which is restricted to administrators. The TOE does not provide any mechanism for users to modify audit records.
FDP_IFC.1	**Policy Enforcement** – The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is handled inappropriately.
FDP_IFF.1	**Policy Enforcement** – The TOE implements data classification to identify/track sensitive data and Protection Rules to act when sensitive data is handled inappropriately.
FIA_ATD.1	**Management** – User security attributes are associated with the user user account via ePO User Account management.
FIA_UID.1	**Identification** - The TSF requires users to identify and authenticate themselves before invoking any other TSF function or before viewing any TSF data via an interface within the TSC. No action can be initiated before proper identification and authentication.

SFR	SF AND RATIONALE
FIA_USB.1	**Identification** - Upon successful login, the TOE binds the Global Administrator status and the union of all the permissions from the permission sets from the user account configuration to the session.
FMT_MTD.1	**Management** – The Global Administrator status and user permissions determine the access privileges of the user to TOE data.
FMT_SMF.1	**Management** – The management functions that must be provided for effective management of the TOE are defined and described.
FMT_SMR.1	**Management** – The TOE provides the roles specified in the SFR. When a User Account is created or modified, the role is specified by setting or clearing the Global Administrator status for the user.
FPT_TDC.1	**System Information Import** – The TOE provides the functionality to import asset data information from Active Directory (LDAP servers) or NT Domains and correctly interpret the information.

Table 24 – SFR to TSF Rationale

7 TOE Summary Specification

7.1 Policy Enforcement

The TOE protects sensitive information from being disclosed through various channels, including email, print, or copy to an external storage device. Protection rules control the flow of data by defining the action taken when an attempt is made to transfer or transmit sensitive data. Protection Rules link actions with definitions, tags and content categories, and user assignment groups.

Protection rules define the action taken when an attempt is made to transfer or transmit tagged data. The protection rule specifies the transfer method, named tag(s), and how the system should react to the event. Each event is given a severity level, and options for responding to the event. In some cases, protection rules merely log the event. In other cases, the protection rules may prevent the transfer of data and notify the user of the violation. Protection rules are optionally applied to assignment groups. This allows a rule to apply only to particular user groups.

ACTIONS RULES	Apply RM Policy	Block	Encrypt	Delete	Monitor	Notify User	Quarantine	Read Only	Request Justification	Store Evidence
Plug and Play device rules		✓			✓	✓				
Removable storage device rules		✓			✓	✓		✓		
Application file access protection rules					✓	✓				
Clipboard protection rules		✓								
Email protection rules		✓			✓	✓			✓	✓
File system protection rules			✓		✓	✓				✓
Network communication protection rules		✓			✓	✓				
PDF/Image Writer protection rules		✓			✓	✓				
Printing protection rules		✓			✓	✓				✓
Removable storage protection rules		✓	✓		✓	✓				✓
Screen capture protection rules		✓			✓	✓				✓
Web post protection rules		✓			✓	✓			✓	✓
Discovery rules	✓		✓	✓	✓		✓			✓

Table 25 – Rules and their actions

After creating the rules and definitions required for the enterprise, they must be enforced by assigning the policy to managed computers. Once the policy is in place, the Host DLP Monitor is used to audit the state of the enterprise's sensitive information.

Using McAfee Host Data Loss Prevention software involves the following tasks:

- Assigning policy — Deploying the Host DLP policy to managed computers.
- Monitoring events — Using the Host DLP Monitor to audit, view, filter, and sort events in the enterprise network.
- Performing administrative maintenance — Keeping the DLP Agents up-to-date and generating agent override, agent uninstall, and quarantine release keys as required.

The table below shows the predefined dashboards and available functions for the Policy Enforcement TSF:

NAME	DESCRIPTION
Agent Distribution by Date	Displays how many agents are installed per day.
Agent version	Displays the distribution of agents in the enterprise. Used to monitor agent deployment progress.
Bypassed agents	Displays how many Host DLP nodes are in policy bypass mode. This is a real-time view that refreshes when a bypass begins or expires.
Enforced Device Control Rules	Displays the number of computers enforcing each device control rule. Drill down to view which rules are being enforced on which users.
Enforced Protection Rules	Displays the number of computers enforcing each protection rule.
Event collector distribution	Shows how many nodes report to each event collector server. Useful in the case of a multiple event collector setup.
Evidence Path Distribution	Displays the different evidence shares used by the agents. Useful when there are several different agent configurations.
Policy Distribution	Displays the Host DLP policy distribution throughout the enterprise. Used to monitor progress when deploying a new policy.
Privileged Permissions	Displays the current privileged Host DLP users. It allows drill down to view normal Host DLP users as well as users with “monitor only” permissions, and users allowed to bypass all Host DLP events.

Table 26 – Predefined DLP Dashboards

7.2 Identification

Users must log in to ePO with a valid user name and password supplied via a GUI before any access is granted by the TOE to TOE functions or data. When the credentials are presented by the user, ePO determines if the user name is defined and enabled. If not, the login process is terminated and the login GUI is redisplayed.

The supplied password is passed to Windows for validation. If it is successful, the TOE grants access to additional TOE functionality. If the validation is not successful, the login GUI is redisplayed. Note that all the Windows I&A protection mechanisms (e.g., account lock after multiple consecutive login failures) that may be configured still apply since Windows applies those constraints when performing the validation.

Upon successful login, the Global Administrator status and the union of all the permissions from the permission sets from the user account configuration are bound to the session. Those attributes remain fixed until the user refreshes their session.

7.3 Management

The TOE's Management Security Function provides administrator support functionality that enables a user to configure and manage TOE components. Management of the TOE may be performed via the ePO GUI. Management permissions are defined per-user.

The TOE provides functionality to manage the following:

1. ePO User Accounts,
2. Permission Sets,
3. Audit Log,
4. Event Log,
5. Notifications,
6. Event Filtering,
7. System Tree,
8. DLP Policies and Rules,
9. Queries,
10. Dashboards.

Each of these items is described in more detail in the following sections.

7.3.1 ePO User Account Management

Each user authorized for login to ePO must be defined with ePO. Only Global Administrators may perform ePO user account management functions (create, view, modify and delete). For each defined account, the following information is configured:

1. User name
2. Enabled or disabled
3. Whether authentication for this user is to be performed by ePO or Windows (the evaluated configuration requires Windows authentication for all users)
4. Permission sets granted to the user
5. Global Administrator status

One or more permission sets may be associated with an account. Global Administrators are granted all permissions.

Permissions exclusive to global administrators (i.e., not granted via permission sets) include:

1. Change server settings.
2. Create and delete user accounts.
3. Create, delete, and assign permission sets.
4. Limit events that are stored in ePolicy Orchestrator databases.

7.3.2 Permission Set Management

A permission set is a group of permissions that can be granted to any users by assigning it to those users' accounts. One or more permission sets can be assigned to any users who are not global administrators (global administrators have all permissions to all products and features).

Permission sets only grant rights and access — no permission ever removes rights or access. When multiple permission sets are applied to a user account, they aggregate. For example, if one permission set does not provide any permissions to server tasks, but another permission set applied to the same account grants all permissions to server tasks, that account has all permissions to server tasks.

When a new ePO product extension (e.g., HDLP) is installed it may add one or more groups of permissions to the permission sets. Initially, the newly added section is listed in each permission set as being available but with no permissions yet granted. The global administrators can then grant permissions to users through existing or new permission sets.

Global administrators may create, view, modify and delete permission sets. Each permission set has a unique name so that it can be appropriately associated with ePO users.

When a permission set is created or modified, the permissions granted via the permission set may be specified by a global administrator.

7.3.3 Audit Log Management

A global administrator may configure the length of time Audit Log entries are to be saved. Entries beyond that time are automatically purged. If the database space is exhausted, new entries are discarded and an SNMP trap is generated.

7.3.4 Event Log Management

A global administrator may configure the length of time DLP policy audit event records are to be saved. Entries beyond that time are automatically purged.

The DLP policy audit event records may also be purged manually by a global administrator using a GUI to specify that all events older than a specified date are to be deleted. This is a one-time operation and the date specified is independent of the time period specified for automatic purging.

7.3.5 Notification Management

Notifications may be specified in response to events generated by the TOE. Notifications cause email messages to be sent to the configured recipient(s) or SNMP traps to be generated.

A global administrator may configure the SMTP server name and port used to send email or the destination(s) for SNMP traps. Credentials may optionally be specified if authentication is to be performed with the email server.

A global administrator or user with the “Create and edit contacts” permission may create, view, edit and delete contacts. Each contact includes a first name, last name and email address. The contacts are used in email notifications; any global administrator or user with the “Use contacts” permission may cause a notification to be sent to the specified contact for that notification.

A global administrator or user with the appropriate permissions (see below) may configure independent rules at different levels of the System Tree. The rules specify when and what type of notification should be sent under what conditions.

The permissions associated with Notification management are:

1. View notification rules and Notification Log - This permission also grants the ability to view SNMP servers, registered executables, and external commands.
2. Create and edit notification rules; view Notification Log - This permission also grants the ability to view SNMP servers, registered servers, and external commands.
3. Create and edit notification rules; view and purge Notification Log; create and edit SNMP servers and external commands

The sending of notification messages can be configured by setting thresholds based on aggregation and throttling. Aggregation determines the thresholds of events at which the rule sends a notification message. Once the rule is configured for notification, throttling can contain the number of notification messages.

Once associated with a group or system, notification rules may be enabled and disabled by a global administrator or user with the “Create and edit contacts” permission.

7.3.6 Event Filtering Management

A global administrator may view and modify the list of events that are forwarded from the agents to the ePO server. The list of events is common to all agents.

7.3.7 System Tree Management

The System Tree organizes managed systems in units for monitoring, assigning policies, scheduling tasks, and taking actions. The System Tree is a hierarchical structure that allows organization of systems within units called groups.

Groups have these characteristics:

1. Groups can be created by global administrators or users with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.
2. A group can include both systems and other groups.
3. Groups are modified or deleted by a global administrator or user with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.

The System Tree root includes a Lost&Found group. Depending on the methods for creating and maintaining the System Tree, the server uses different characteristics to determine where to place systems. The Lost&Found group stores systems whose locations could not be determined.

The Lost&Found group has the following characteristics:

1. It can't be deleted.
2. It can't be renamed.
3. Its sorting criteria can't be changed (although sorting criteria for subgroups can be created)
4. It always appears last in the list and is not alphabetized among its peers.
5. All users with view permissions to the System Tree can see systems in Lost&Found.
6. When a system is sorted into Lost&Found, it is placed in a subgroup named for the system’s domain. If no such group exists, one is created.

Child groups in the System Tree hierarchy inherit policies set at their parent groups. Inheritance is enabled by default for all groups and individual systems that are added to the System Tree. Inheritance may be disabled for individual groups or systems by a Global Administrator. Inheritance can be broken by applying a new policy at any location of the System Tree (provided a user has appropriate permissions). Users can lock policy assignments to preserve inheritance.

Groups may be created manually or automatically (via synchronization with Active Directory or NT Domains). Systems may be deleted or moved between groups by a Global Administrator or user with both the “View "System Tree" tab” and “Edit System Tree groups and systems” permissions.

7.3.8 DLP Policy Management

A product policy is a collection of settings that are created, configured, and then enforced. Product policies ensure that McAfee Agent and HDLP are configured and perform accordingly on the managed systems. Different product policies for the same product may be configured for different groups. When product policy settings are reconfigured, the new settings are delivered to, and enforced on, the managed systems at the next agent-server communication.

The permissions associated with product policy management are:

1. View settings (McAfee Agent) - This permission grants the ability to view settings for the McAfee Agent product policy.

2. View settings (HDLP Agent) - This permission grants the ability to view settings for the HDLP Agent product policy.
3. View and change settings (McAfee Agent) - This permission grants the ability to view, create, delete, enable and modify settings for the McAfee Agent product policy.
4. View and change settings (HDLP Agent) - This permission grants the ability to view, create, delete, enable and modify settings for the HDLP Agent product policy.

Product policies are applied to any group or system by one of two methods, inheritance or assignment. Inheritance determines whether the product policy settings for a group or system are taken from its parent. By default, inheritance is enabled throughout the System Tree. When this inheritance is broken by assigning new product policies anywhere in the System Tree, all child groups and systems that are set to inherit the product policy from this assignment point do so. A Global Administrator can assign any product policy in the Policy Catalog to any group or system. Assignment allows the definition of product policy settings once for a specific need and then the application of the product policy to multiple locations.

All product policies are available for use by any user, regardless of who created the product policy. To prevent any user from modifying or deleting other users' named product policies, each product policy is assigned an owner — the user who created it. Ownership provides that no one can modify or delete a product policy except its creator or a global administrator. When a product policy is deleted, all groups and systems where it is currently applied inherit the product policy of their parent group.

Once associated with a group or system, enforcement of individual product policies may be enabled and disabled by a global administrator.

7.3.9 Query Management

Users may create, view, modify, use and delete queries based upon their permissions. Permissions associated with queries are:

1. Use public queries — Grants permission to use any queries that have been created and made public.
2. Use public queries; create and edit personal queries — Grants permission to use any queries that have been created and made public by users with the same permissions, as well as the ability to create and edit personal queries.
3. Edit public queries; create and edit personal queries; make personal queries public — Grants permission to use and edit any public queries, create and modify any personal queries, as well as the ability to make any personal query available to anyone with access to public queries.

7.3.10 Dashboard Management

User-specific dashboards may be configured to display data of interest to each user; these chart-based displays are updated at a configured rate to keep the information current. Permissions relevant to dashboards are:

1. Use public dashboards
2. Use public dashboards; create and edit personal dashboards
3. Edit public dashboards; create and edit personal dashboards; make personal dashboards public

7.4 Audit

The Audit Log maintains a record of ePO user actions. The auditable events are specified in Table 16 – Audit Events and Details.

The Audit Log entries display in a sortable table. For added flexibility, the log can be filtered so that it only displays failed actions, or only entries that are within a certain age. The Audit Log displays seven columns:

1. Action — The name of the action the ePO user attempted.
2. Completion Time — The date and time the action finished.
3. Details — More information about the action.
4. Priority — Importance of the action.
5. Start Time — The date and time the action was initiated.
6. Success — Specifies whether the action was successfully completed.
7. User Name — User name of the logged-on user account that was used to take the action.

Audit Log entries can be queried against by a Global Administrator or users with the “View Audit Log” permission. The Audit Log entries are automatically purged based upon a Global Administrator-configured age. Other than automatic purging, no mechanisms are provided for users to modify or delete entries. The audit log entries are stored in the database; if space is exhausted, new entries are discarded.

Additionally, the TOE provides the following DLP Information Flow Control SFP events:

NAME	DESCRIPTION
Block and Block Write Device Events	Displays device events that were blocked or write-blocked.
Daily Events distribution by Severity	Displays a day's events ordered by severity.
Enforced Discovery Rules	Displays the number of computers enforcing each discovery rule.
Events by Event Type	Displays the number of events for each event type

NAME	DESCRIPTION
Events by Protection/Discovery Rule by Date	Displays the number of events for each rule, for different dates.
Events by Protection Rule	Displays the number of events for each rule.
Events by Severity	Displays the number of events for each severity level.
Events by Tag and Category	Displays the number of events for each tag and content category that they recognize.
Undefined Device Classes	Lists and shows a bar graph of the devices whose device class cannot be determined.
Unmanaged Printers	Lists and shows a bar graph of the unmanaged (whitelisted) printers and the number of nodes attached to each. Clicking either a listed printer or a bar on the graph drills down to a list of the computers connected to it. Clicking on a computer drills down to the properties of the computer.

Table 27 – Predefined DLP Event Reports

7.5 System Information Import

ePO offers integration with both Active Directory and NT domains as a source for systems, and even (in the case of Active Directory) as a source for the structure of the System Tree.

Active Directory synchronization can be used to create, populate, and maintain part or all of the System Tree with Active Directory synchronization. Once defined, the System Tree is updated with any new systems (and subcontainers) in Active Directory.

There are two types of Active Directory synchronization (systems only and systems and structure) that can be used based on the desired level of integration with Active Directory.

With each type, the following synchronization options are available:

1. Deploy agents automatically to systems new to ePolicy Orchestrator.
2. Delete systems from ePolicy Orchestrator (and remove their agents) when they are deleted from Active Directory.
3. Prevent adding systems to the group if they exist elsewhere in the System Tree.
4. Exclude certain Active Directory containers from the synchronization. These containers and their systems are ignored during synchronization.

The System Tree can be populated with the systems in the NT domain. When synchronizing a group to an NT domain, all systems from the domain are put in the group as a flat list. Those systems can be managed in a single group or via subgroups for more granular organizational needs.

When systems are imported, their placement in the System Tree may be automatically determined by criteria-based sorting of two forms. IP address sorting may be used if IP address organization coincides with the management needs for the System Tree. Tag based sorting may be used to sort systems based on tags associated with them.

The server has three modes for criteria-based sorting:

1. Disable System Tree sorting
2. Sort systems on each agent-server communication — Systems are sorted again at each agent-server communication. When the sorting criteria on groups is changed, systems move to the new group at their next agent-server communication.
3. Sort systems once — Systems are sorted at the next agent-server communication and marked to never be sorted again.